Was ist ein sicherer Hoster und wie wähle ich diesen aus?

Intention

Dieses Pattern bietet eine Auflistung von Punkten, die ein Webhoster erfüllen sollte, um als sicher eingestuft zu werden.

Problemstellung

Es gibt Webhoster wie Sand am Meer, doch nicht jeder ist automatisch sicher. Der Hoster kann subjektiv als gut empfunden werden, weil es scheint, dass die Leistungen und der Preis stimmen. Der Standort spielt bezüglich Sicherheit und Erreichbarkeit eine wichtige Rolle.

Szenario

Die Website steht und liegt lokal auf dem Computer. Nun benötigt man einen Webhoster um diese Online stellen zu können. Es gibt viele Anbieter von Webhostern, aber wie trifft man die richtige Wahl?

Lösung

Auf folgende Punkte muss **man bei der Wahl eines sicheren Webhosters achten:**

- Keine gratis Lösungen verwenden
    - Webhoster müssen sich auf eine Weise finanzieren. Dies erreichen sie mittels Werbeanzeigen auf der gehosteten Seite oder durch andere Mittel. Kunden haben keinen Einfluss auf die Werbung und deren Quelle, somit ist es nicht ratsam solch einen Hoster zu wählen. Die Werbung könnte auch Schadcode oder Schadprogramme über ihre Seiten verteilen.
    - Daher gibt es keine Empfehlung für Webhoster, die den Service unentgeltlich anbieten.
- Update-Garantie beachten
    - Seriöse und sichere Hosting-Services erkennen Sie an deren Bereitschaft, dass zur Verfügung gestellte System und die Software aktuell zu halten. Aktuelle Systeme bieten weniger Angriffsfläche für Hacker.
- SSL-Zertifikate

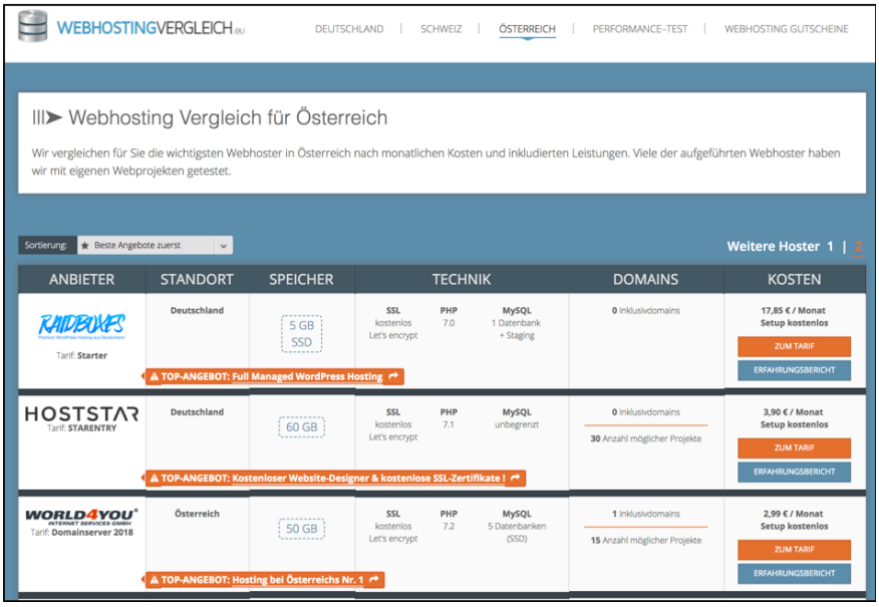
    - HTTPS ist ein Muss, wenn es um die Sicherheit und die Datenintegrität geht. Deshalb sollte bei der Auswahl eines Webhosters darauf geachtet werden, ob dieser SSL-Zertifikate ausstellt oder zumindest die Möglichkeit bietet Zertifikate selbst zu erstellen und diese auch einzubinden.
- DDoS-Protection
    - Dieser Punkt ist vor allem dann wichtig, wenn die Seite immer verfügbar sein sollte. Denn dann kann auch im Fall der Fälle der Webhoster dafür sorgen, dass die Seite während eines DDoS-Angriffs verfügbar oder gesichert ist.
- Standort des Hosters
    - Sofern mit personenbezogenen Daten gearbeitet wird sollte man sich Gedanken machen wo der Server steht.

Die nachfolgenden Punkte sind *optional* und man kann sie auch eigenständig abdecken, dennoch erhöhen sie die Sicherheit und erleichtern einem die Arbeit:

- Malware Scan / Spam Überprüfung / XSS Überprüfung / Viren Scan
    - Webhoster überprüfen die Seite regelmäßig. Es wird geprüft ob die von ihnen gehosteten Seiten Schadsoftware verteilen oder sie auf bestimmten Verdachts- oder Blacklists stehen.
- Backups
    - Dieser Punkt ist zwar *optional*, wenn man diese selbst durchführt, doch wenn der Webhoster zusätzlich Backups durchführt, ist dies von Vorteil.

Beispiele

Vergleich von Webhostern aus Deutschland, Österreich und der Schweiz: https://www.webhostingvergleich.eu/at/oesterreich/



Da der Markt sich ständig ändert, sollte man immer nach dem aktuellsten Ranking suchen und vergleichen. Vor allem Aspekte wie Sicherheit, Preis und Dienstleistungen können sich erheblich unterscheiden.

SSL / TLS Verschlüsselung

Im Pattern „**Wie verschlüssele ich die Kommunikation mit meiner Website?**“ wird erklärt wie man eine *SSL / TLS* Verschlüsselung auf der eigenen Seite integriert. Mit der sicheren HTTPS-Verbindung geschieht die Kommunikation zwischen dem Webbrowser des Nutzers und der verschlüsselten Website. Somit kann sicher gegangen werden, dass alle Daten, die vom Nutzer stammen auch von ihm sind.

DDoS Attacken

Das Pattern „**Was kann man gegen DDoS Attacken tun?**“ befasst sich mit der Thematik der DoS- und DDoS-Attacken und was man gegen diese Unternehmen kann.

Sich selbst um Sicherheit und Backups kümmern

Man sollte die Sicherheit der Website unter allen Umständen gewährleisten. Wenn man auf die optionalen Angebote des Webhosters verzichtet, kann man sich auch selbst darum kümmern. Wie das geht, wird in den Patterns „**Was trägt alles zur Sicherheit einer Website bei?**“, „**Wann und wie sollte man Backups erstellen?**“, „**Wie speichere ich Daten von Websitebesuchern sicher?**“, „**Welche Daten darf ich auf meiner Website speichern?**“, sowie „**Welche Informationen muss ich den Besuchern auf meiner Website bereitstellen?**“ erklärt.

Referenzen

https://www.thesitewizard.com/archive/findhost.shtml
https://webdesign.tutsplus.com/tutorials/the-seriously-comprehensive-guide-to-choosing-a-web-host–cms-25430

Keywords

Webhoster, Sicherheit